Research Report

This report has been compiled using a combination of publicly available data and data collected from Lepide Risk Assessments.

Lepide

The State of Active Directory Security:

Key Risks to Monitor for 2025

Learn more about Lepide

https://www.lepide.com

Introduction

The threats organizations face in 2025 have changed considerably from even a couple of years ago. Active Directory (AD) has and still is, one of the most overlooked areas of cybersecurity. AD is the central part of identity and access management where users are authenticated and permissions to systems are established. As a result, AD is often the subject of scrutiny by attackers who are trying to exploit misconfigurations, excessive permissions and visibility gaps.

In this report, we will discuss the current state of AD security and point out the top risks organizations will need to address in the upcoming year in order to avoid making the headlines. We will explore 10 risk factors related to AD security such as admin users, inactive accounts, permission changes and failed logons. We provide insights into the associated risks for each, along with recent data and analysis from experts. We also provide recommendations for remediating those areas of risk.

As the CEO of Lepide, a company committed to helping organizations secure their most valuable digital assets, I believe that understanding and proactively addressing the security gaps in Active Directory is essential for maintaining the integrity of your IT environment. The insights in this report will equip you with the knowledge and tools needed to fortify your Active Directory infrastructure and protect your organization from the ever-growing range of cyber threats.

Aidan Simister
CEO, Lepide

About this report

The goal of this report is to help identify ten important, measurable indicators in Active Directory, which are closely linked to risk, for example, inactive users, admin accounts, permission changes, and failed logins. Using public data and our customers' experience, we highlight the risks associated with inadequate management of these indicators, and provide ways to remediate them. By focusing on these important vulnerabilities, we help security teams, IT administrators and business leaders concentrate their efforts on the most important ways to reduce exposure to threats in 2025 and beyond.

In this report, we will go through:

1. User accounts
2. Admin users
3. Inactive users
4. Users with passwords set to never expire
5. Permission changes
6. Password policy changes
7. Failed logons
8. Account lockouts
9. Activity outside of business hours
10. User/computer status changes

The Hidden Cost of Inaction:

Inside the AD Mismanagement Crisis Plaguing Data Security

A newly released study of Active Directory and identity management behaviors suggests a deeply concerning pattern of negligence, inefficiencies, and risk for organizations of all types. Some of the key takeaways are:

- **Excessive permissions are a fact of life**: 79% of organizations have users with excessive privileges, creating unnecessary surfaces for attack.
- **Orphaned & inactive accounts are out of control**: Up to 30% of corporate accounts are inactive or orphaned accounts -- small ticking time bombs of breach potential.
- **Password practices are actively dangerous**: 45% of organizations have outdated or weak password policies in place, while 23% have users with "never expires" settings.
- **Access chaos leads to breaches and downtime**: Unauthorized changes, as well as users with improper permissions, account for 25% of breaches, while 43% of organizations experience frequent account lockouts.

Insiders and After-Hours Activity Are Forms of Serious Risk: Insider access is responsible for 33% of incidents outside of business hours, while 25% of organizations detect suspicious activity outside of typical business windows.

These failures often are not just risks of potential breaches - they have cost our business £4 million in disruption in just over the last two years due to ransomware attacks that benefit from failed admin controls.

As stated before, the recommendation is clear: Organizations must regain control of their Active Directories before the next breach is from an inside job.

- **79% of organizations have users with "excessive permissions"**, indicating a lack of stringent control over admin access.
- **Proliferation of admin accounts has led to £4 million worth of disruption to businesses in the last two years** due to incidents like ransomware attacks exploiting admin accounts.
- **21% of Active Directory accounts** within organizations were either **inactive** or had been **abandoned**.
- Improper permission settings or unauthorized permission changes were responsible for **25% of data breaches.**
- **45% of organizations** are found to have **outdated or weak password policies**, which could leave them vulnerable to common attack methods like brute force or credential stuffing.
- **Failed logon attempts** are linked to nearly **40% of data breaches** involving external actors.
- **43% of organizations** report **frequent account lockouts**, leading to substantial downtime and administrative burden.
- **33% of cybersecurity incidents** were caused by insiders accessing systems **outside of business hours**.

1. User accounts.

According to Statista and Microsoft estimates, **over 95%** of Fortune 1,000 companies use Active Directory for identity and access management.

By collating data from multiple surveys with data from Microsoft, we estimate the following for Active Directory user counts by company size:

🔍 Many AD environments contain **2–3× more user accounts than actual employees**, due to contractors, ex-employees, test users, and service accounts.

Employee Range	Estimated Average AD Users	Notes
1–250	150–300	Smaller organizations often have a near 1:1 ratio of employees to AD users, with additional accounts for service users and contractors.
251–500	400–700	Medium-sized businesses may have more complex structures, leading to a higher number of AD accounts relative to employees.
501–1,000	800–1,500	Growth in departments and services increases the number of user accounts, including service and administrative accounts.
1,001–2,500	1,800–3,500	Larger organizations often have multiple domains or forests, contributing to higher AD user counts.
2,501–10,000	4,000–15,000	Enterprises in this range may include multiple subsidiaries or global branches, each adding to the total AD user count.
10,000+	20,000+	Very large enterprises can have extensive AD infrastructures, sometimes exceeding 100,000 user accounts, especially when considering service accounts and external collaborators.

1. User accounts.

⚠️ Associated Risks

Attack surface bloat:

The more user accounts an organization has in Active Directory, the more possible entry points an attacker has. Each account — whether used every day or forgotten about — is another set of credentials that can be stolen, guessed, or phished. Most security teams focus on privileged accounts, but even a standard user account can lead to initial access, lateral movement, and privilege escalation.

Large AD environments, and especially ones that haven't been audited frequently, often have test accounts, old contractor accounts, and legacy service accounts that remain with valid credentials. These accounts often go unnoticed and are not part of MFA, or even adhere to any robust password policies. As attackers rely more on living-off-the-land techniques, the more accounts that are present means the likelihood increases that someone can take advantage of one, at some level.

Audit and compliance challenges:

Managing a large number of AD user accounts creates complications for IT and security teams. Each account is subject to lifecycle management, group membership, access control, and monitoring and alerting. As the number of users in an AD environment grows, so too do the chances for misconfigurations—such as stale group memberships, overlapping permissions, or mismanaged service accounts.

In large AD environments, it is harder from an accountability perspective to know who has access to what. Rules and regulations that govern data, such as GDPR, HIPAA, SOX, and ISO 27001, expect organizations to have process controls over who has access to what. Without reviews and automated tooling, it can be difficult to prove that you do and how you keep it under control. The risks are not just technical; they are also regulatory and reputational.

Privilege creep:

As users gain positions and transition in and out of roles, they typically accumulate more access than they can use given their current job role. Employees change roles, and employees join projects on a temporary basis, while often gaining permissions that are rarely revoked. As organizations escalate the number of users across their AD, it becomes much more apparent that the variable's employees and/or user base have excessive access due to an unlimited number of permissions being granted.

The act of stacking permissions across their tenure at an organization becomes "privilege creep" or excessive rights beyond any job-related functions. The problem with over-permissioning is that it violates even the most basic sense of "least-privilege" whereby there is potential for both internal abuse and external abuse. If an attacker compromises an overly privileged account, the attacker may get more access and have fewer identifiers than they would otherwise. Large environments suffer from a lack of visibility into permissions and relationships across identities, elevating the risks and making it harder to detect when there are misalignments.

1. User accounts.

🛡️ How to Mitigate the Risk

Implement automated user lifecycle management:

Automating the provisioning and deprovisioning process for user accounts is one of the best things an organization can do to mitigate potential risk. Doing this through integration of AD with your HR platform or identity governance platform will result in the automatic creation, modification and deactivation of accounts based on the employment status of the employee.

Automation will also help ensure consistency in account creation so users are added to the proper groups and only have the permissions they are entitled to based on their roles. This reduces human error and speeds up the onboarding and offboarding cycles. If a user has a role change, their access can be systematically reviewed and changed, which can support least privilege and slow down access sprawl.

Conduct regular access reviews and cleanups:

Regular access reviews are Important for keeping account privileges in line with job responsibilities. For a review to be effective, it involves more than Just the IT or security teams, it also involves the department managers who know which access their teams actually need. When considering their Teams, departments should review user group memberships, roles, and login activity, this can help discover stale accounts, unjustified privilege, and potentially suspicious changes.

In addition to regular reviews, organizations should also take part in regular clean-up exercises, like, disabling accounts that haven't been used in 30/60/90 days, removing users from groups that are inactive or unused, and/or deleting dead or defunct service accounts.

There are many tools for AD management that can automate these audits and identify anomalies, helping to create a leaner, safer environment.

Enhance Monitoring and Alerting:

There should be a comprehensive monitoring of account activity as a part of managing AD and its users, especially in larger AD environments, where it's nearly impossible to oversee manually. Organizations should find a means to monitor volume and changes to accounts, group memberships and account permissions in near real-time. Alerting on different patterns of unusual behaviors (e.g., a user added to multiple admin groups or they log in outside of standard hours) could help identify threats early.

Log information from AD should be reviewing with a SIEM or security analytics platform to identify potential patterns of compromise that could reveal unauthorized activity; examples include brute-force attempts, privilege escalation and/or lateral movement. In high-volume environments with many accounts (e.g. corporate account structure, contractor roles), it places more emphasis on organizations maintaining visibility; all accounts should be seen as potential blind spots.

2. Admin users.

📊 Key Statistics

Prevalence of Admin Accounts:

- A significant number of organizations grant administrative privileges to a substantial portion of their workforce. Lepide has revealed through their Risk Assessment program that **79% of organizations have users with "excessive permissions"**, indicating a lack of stringent control over admin access.

Financial Impact of Excessive Admin Privileges:

- The proliferation of admin rights has been identified as a catalyst for business disruptions. One study highlighted that such practices have cost organizations over **£4 million in the last two years** due to incidents like ransomware attacks exploiting admin accounts.

⚠️ Associated Risks

Expanded attack surface:

If an attacker compromises an admin account, they often have access to the entire environment which may include sensitive data, configuration settings to change security fundamentals, or the ability to launch malicious software. When organizations have a considerable number of admin users, the risk of admin accounts being easily compromised grows exponentially because there will be numerous accounts that may not have been secured or monitored adequately. Attackers could simply exploit these admin vulnerabilities from weak passwords, social engineering, or even lack of MFA in order to get access.

Many organizations do not assign adequate monitoring to the activities conducted by all admin users, enabling the repeated ability of attackers to go undetected for a long duration of time. Once an attacker manages to compromise an admin account, they can use the access to escalate their privileges, move laterally in the network, and potentially exfiltrate sensitive information. Lastly, it also does not help that there are so many admin accounts which reminds be of the adage that "the more doors, the more entry points" - the more admin accounts, the more potential attack vectors that an organization has to monitor and prioritize as opposed to the actual risk.

Organizational disruption:

The risk of unauthorized changes to important systems and configuration increases with admin rights. Such changes may seriously disrupt services or operations. For example, a user with admin rights may make a change to a system without any malicious intent that causes instability and discontinues operations.

2. Admin users.

⚠️ Associated Risks (continued)

or accidently install software that conflicts with other business-critical applications. If an attacker obtains access to an admin account, they could perform acts of sabotage that could result in downtime, data corruption, or even failure of the core system that would impact the entire organization.

Organizations may experience delayed incident detection and recovery in notice due to their complexity with admin access model. When different admin users have conflicting permissions or inconsistent access, tracking who made which change could delay the root cause and resolution, extending downtime. For the industries that commonly depend on a high availability and uptime of a core system, downtime during incidents can lead to lost revenue, diminished client trust, and damage the image and reputation of the business.

Regulatory non-compliance:

Regulatory requirements around access control, data protection, and user management can be very stringent for many industries, especially those that involve sensitive data (e.g., healthcare, finance, and government). An organization which poorly manages admin accounts, for example permitting excessive admin rights, or fails to enforce sufficient access control standards may be vulnerable to compliance violations. Regulatory frameworks, such as GDPR, HIPAA and SOX, typically require the organization to allow access to sensitive systems and data by only authorized users, but the framework typically does not specify how that access must be controlled or monitored.

Failing to comply with these regulatory requirements could result in severe penalties (e.g., financial punishments or damage to the organization's reputation). Additionally, compliance auditors will regularly review the management of privileged accounts as part of their audits, therefore non-compliance related to admin account management could lead to lost audits. Hence, it is critical for organizations to have solid access management processes in place to meet compliance from all relevant standards.

Mitigation Strategies

Implement the Principle of Least Privilege (PoLP):

One of the most effective ways to mitigate the risks associated with admin users is to implement the principle of least privilege (PoLP), which dictates that users should only be granted the minimum level of access necessary for them to perform their job functions. For admin accounts, this means that only users who genuinely need administrative access should have it, and even then, their permissions should be as restrictive as possible. For example, an admin user should only have access to the systems or data required for their responsibilities and should not have global admin rights across the entire AD environment.

To enforce this principle, organizations should regularly review and audit the roles and responsibilities of admin users. This helps ensure that over time, as users change roles or responsibilities within the company, their access permissions are adjusted accordingly. Furthermore, temporary admin rights

2. Admin users.

Mitigation Strategies (continued)

For specific tasks or for certain time periods, restrictions should be put in place to prevent users from maintaining unnecessary access. This approach should minimize the damage from either a compromised admin account or an admin user making an honest mistake.

Utilize Role-Based Access Control (RBAC):

Role-Based Access Control (RBAC) is a useful method of managing admin rights, by assigning permissions using a set of definable roles in the organization. Administrators can assign users to specific roles with associated permissions instead of just writing wider administrative privileges to users. Roles can be based on job functions (e.g. "System Administrator," "Network Administrator," "Security Officer"), and will have access to only those resources and tools necessary to perform the functions of their role.

Using roles allows organizations to establish a more granular level of control over admin privileges. Moving from a situation where all users have access to certain administrative capabilities to limiting this access to a few users will have a far-reaching impact on the organization. Using this access approach will also help track which users have access to specific systems, as well as allow for ease of blocking access when the user's admin role changes, or they leave the organization. Furthermore, RBAC can help organizations that have regulatory requirements by ensuring that the right people have access to critical systems, and to produce audit logs that show who accessed what when.

Separate administrative and user accounts:

A frequent curse in many organizations is that users perform both typical user tasks and administrative tasks in the same account. This encourages a cavalier attitude towards the enormous privilege granted. Users are more likely to use their admin accounts in any situation that requires them to perform their normal everyday tasks. As a result, they are much more likely to accidentally change a system configuration using admin privileges than to make the same mistake if using their normal user account. Moreover, separating administrative and user accounts creates a clear difference between normal day-to-day usage and privilege access tasks, and that separation significantly lowers that risk.

If a user has normal and admin account, it is much easier to know what actions were performed with elevated privileges. Separating accounts also ensures that if an account is compromised, the attacker may only get one level of functionality, not the entire system. Organizations can enforce this by requiring the signing of separate accounts for administrative functions and adding an additional layer of authentication by utilizing multifactor authenticators for users' admin accounts.

3. Inactive users.

📊 Key Statistics

Inactive Accounts Across Organizations:

- According to a report from Gartner, up to 30% of all corporate accounts can be inactive or orphaned, posing significant security risks to organizations.

Average Inactive User Accounts:

- A study by Varonis revealed that 21% of Active Directory accounts within organizations were either inactive or had been abandoned. This highlights the prevalence of unused or forgotten accounts.

⚠️ Associated Risks

Security breaches due to orphaned accounts:

Dormant accounts can be important assets to criminals, especially if they belong to a past employee or contractor, since they still have access privileges, and perhaps the privilege of a system administrator or department head, even if the individual is no longer in a role that requires access.

requires them. Cyber attackers can take advantage of these unused accounts to gain unauthorized access, bypassing current user credentials and security practices. Inactive accounts are not subject to much scrutiny, so they can stay around a long time in the system and are often a favorable target for attackers. An attacker can compromise the network through these accounts, perform privilege escalation, and then escalate the attack to cause even more damage.

Inactive accounts are largely unmonitored so they can build up in your environments over time. The longer you leave an account inactive, the greater the chance it can become a path for attack. Attackers can take advantage of inactive accounts in a myriad of ways, including lateral movement, access sensitive data, impacting business continuity to critical software settings.

Non-compliance with regulations and standards:

Numerous regulations (such as GDPR, HIPAA, and SOX) require a business to ensure that access to sensitive systems and data is strictly controlled and periodically reviewed. If many inactive accounts exist, non-compliance could occur. For example, GDPR states access to personal data must be limited to those employees with a need to know due to their job responsibilities. If an inactive account retains access to sensitive data, it might accidentally lead to a data breach and may be subject to fines and reputational consequences.

Regulatory bodies assume that organizations have adequate access management and perform regular audits and reviews of access. If accounts remain inactive for longer periods, not only could this lead to breaches and fines, but also reputational risks if it could be classified as violations. Organizations that do not comply with proper management of inactive accounts might be faced with audits and put under scrutiny, as well as possibly required to implement much stricter access management controls and procedures at significant costs.

3. Inactive users.

⚠️ Associated Risks (continued)

Operational risks and increased attack surface:

Inactive accounts (or not having any inactive accounts in an organization with several thousand accounts) can clutter Active Directory, or whatever identity management tool you use, and can create issues for IT teams trying to maintain an accurate and effective system for tracking their active users. The larger the volume of inactive accounts in the system, the more complex the system becomes with ineffective resource management. It also becomes challenging to limit privilege creep and ensure active users have appropriate access. Also, when you add or delete account information, all active users can be affected and possibly any of the inactive users and clutter makes it difficult to provide administrative oversight of accounts. and creates blind spots for your security posture, where you are blind to some accounts that are under active risk.

🛡️ Mitigation Strategies

Automate account deactivation and cleanup:

To limit risks posed by inactive accounts, organizations should implement automation that will deactivate or disable accounts after a defined period of inactivity. This could involve policies that state if an account is not logged into during a defined period—30, 60, 90 days—that account will be disabled or flagged for review. Additionally, there needs to be some level of automated account lifecycle management, so that users are removed or disabled from the system when they leave the company (resignation, termination, or expiration of contract).

By automating this process, it decreases the administrative burden of managing accounts and guarantees that inactive accounts are always cleaned up. Additionally, that will eliminate human error, as people can forget to delete accounts or take some time to get it done. Keeping in mind that we are allowing the process of automatic deactivation, it guarantees that we will conform with security best practices by eradicating the threat of vulnerabilities that go along with not using an account.

Regularly review and audit Active Directory accounts:

Regularly conducting access reviews and audits is vital for managing user accounts (including stale accounts). Organizations should develop and adopt a timeliness to audit Active Directory on a quarterly, semi-annually, or annually basis to find and eliminate inactive accounts. These audits should bring together IT administrators, security personnel, and departmental teams to ensure deactivation and removal processes are completed in accordance with their policies and procedures.

Organizations should verify with audits whether accounts have not been used within a specific period of time and check if accounts belong to users that left the organization or if the users simply have not logged into their accounts in some time. Inactive accounts for former employees or contractors should be marked for removal or deactivation and problems relating specifically to users with privileged access or permissions should be prioritized. In general, publishing a scheduled audit process will identify permissions that may be incorrect or excessive, while reducing access sprawl risk.

3. Inactive users.

Mitigation Strategies (continued)

Implement Multi-Factor Authentication (MFA) and monitoring on sensitive accounts:

While deactivating unused accounts is essential, organizations may also want to consider implementing extra protections for sensitive or privileged accounts that may remain unused, but could still be a major risk. Imposing Multi-Factor Authentication (MFA) requirements on all privileged accounts—even if unused or not login within 90 days—provides an additional safeguard and may make it significantly more difficult for attackers to abuse the accounts if they do gain access. Even if an attacker has active credentials for a long-forgotten admin account, they will not be able to leverage that access without the second factor of authentication (mobile device or hardware token) to perform the action.

In addition to MFA, organizations should also enact real-time monitoring and alerting mechanisms for anomalous use or access attempts on dormant or underused accounts. ALL access attempts on a privileged account should generate alerts for further investigation. Then the organization can choose to mitigate the threat itself, before it turns into an incident. With MFA in place for the account and active monitoring, organizations can limit the exploitability of even unused accounts and significantly reduce their attack surface.

💡 *Tip:* Use solutions like Lepide to automatically identify and clean up inactive users in Active Directory to maintain a reduced threat surface.

Visit: Lepide Active Directory Auditing

4. Users with passwords set to never expire.

📊 Key Statistics

Percentage of Accounts with Never Expiring Passwords:

- Lepide's Risk Assessment program found that 23% of organizations had at least some of their users set to "never expire" for passwords, which could pose a risk to the security posture of those organizations.

Usage of Never Expiring Passwords in Large Organizations:

- According to a report by Verizon, organizations with over 10,000 employees are more likely to use "never expire" settings for certain accounts, particularly for service or system accounts, which can be a security concern due to lack of frequent password updates.

⚠️ Associated Risks

Increased likelihood of credential compromise:

The primary concern that exists for users who use passwords that never expire, revolves around credential theft and misuse. Without consistent password rotations, accounts that are considered 'static' passwords are much more vulnerable to long-term attacks, especially if the password is compromised or weakly formatted. If a password is stolen or disclosed due to phishing, social engineering attempts, or in a data breach, it can continue to be good indefinitely which means the user has unlimited access to resources in question and is not required to re-authenticate.

In administrative or highly privileged account environments where users have static passwords set to never expire, any attacker who gains these credentials has access that could be utilized for months or years. This allows for the lateral movement throughout the environment because of access to internal systems, information or defactionate malware, exfiltrate data or remain/maintains continued presence even if access is blocked through the original entry point. The fewer times passwords are rotated throughout the operational time, the greater the likelihood that an attacker could successfully compromise the system.

Non-compliance with security best practices and regulations:

Some popular security frameworks and compliance regulations (PCI DSS, NIST, CIS Controls) recommend or require regular password changes as a bare minimum requirement for effective security controls. Allowing passwords to go unchanged can position an organization outside of compliance, exposing them to possible audits, penalties, and reputational risk. For example, PCI DSS mandates password changes every 90 days, requiring unpaid credentials to be refreshed regularly.

4. Users with passwords set to never expire.

⚠️ Associated Risks (continued)

From a compliance perspective, Never expiring passwords is a violation of "defense in depth". Organizations should be able to show, through documentation and testing results to auditors and regulators, that they are actively mitigating the risks of account compromise. Not routinely changing passwords could cause an organization to present an internal security risk and also lead to legal and financial consequences if an organization ultimately experiences a data breach, in particular if it is in an industry dealing with sensitive information or in situations where sensitive information could cause damaged reputation or financial ruin.

Password sprawl and management complexity:

When passwords are set to never expire, organizations risk password sprawl. Many times, especially in large environments, long-lived passwords exist without being discovered or maintained at all, which makes the ability to corral and watch passwords increasingly difficult for IT teams when they find themselves with so many untracked and unmonitored credentials.

Furthermore, in accounts with static passwords, the same level of observation and scrutiny may not exist as accounts that require passwords to be changed regularly. This dynamic can lead to untethered password hygiene, and leave the door open for threat actors to exploit. In organizations that may be dependent on automated systems or legacy applications- forcing organizations to not really track passwords or just never reset passwords- the mere absence of manual resets or reassessment of passwords can amplify the inadvertence in the reliability of infrastructure and the password management models used.

🛡️ Mitigation Strategies

Implement regular password expiry policies:

A proven mitigation technique is to enforce password expiry policies across all user accounts. By creating a password expiry timeframe, such as every 30, 60, or 90 days, organizations can ensure that all passwords are changed at least this frequently, to the extent that compromised credentials are allowed to be used by an unauthorized user for a finite period of time. With a stated password expiration policy, passwords cannot be left unchanged indefinitely, mitigating an organization's long-term risk to exploitation.

In the case of service accounts or systems critical to the organization's operations, it's easier to establish better practices by ensuring the use of more secure options like MFA and using a password vault, rather than allowing a situation where the password never expires. An implementation of a password expiry policy lowers the threat of stale passwords, and gives some enforcement in the organization's security policies of routine password updates, while allowing exceptions where deemed appropriate.

Adopt Multi-Factor Authentication (MFA) for sensitive accounts:

Password expiration is a good step toward securing an account, but a better overall account security method is to implement Multi-Factor Authentication (MFA) on every account, especially those with elevated privileges. MFA ensures that when a password is used to build a connection to a secured account, there is an additional factor, like a mobile device or hardware token, that must also be authenticated. MFA makes it exponentially more difficult for malicious actors to gain unauthorized access even if the password was compromised.

4. Users with passwords set to never expire.

Mitigation Strategies (continued)

For accounts with "never expire" passwords - usually service accounts and accounts that have high complexity chains of dependencies due to automated processes - MFA is essential. Whether or not these passwords are static, MFA helps ensure that attackers will not simply account take over these passwords. Requiring MFA across the board for sensitive accounts, in addition to enforcing strong password policies, will greatly improve the organization's security posture - even if you do not have expiration on those passwords.

Use a password vault or management solution:

A password manager allows secure storing of account credentials, managing access, and automating credential change requests for accounts that require static credentials. Organizations can be more proactive about changing passwords for service accounts instead of storing passwords in an easily accessible format, or logging them in a network location without multi-factor authentication. Credential entries and management can be stored comfortably knowing the vault has a schedule or frequency to periodically rotate passwords.

Furthermore, a password vault can work with other security systems to provide visibility and management of who has access to what credentials. While accounts with long-lived passwords may not have a password expiration, a password vault can still manage long-lived passwords, ensuring that they are routinely rotated and monitored. Automating password management with a password manager is typically worth the investment if it helps an organization to reduce password sprawl, improve compliance with security policies, and improve security hygiene in general.

💡 *Tip:* Use solutions like Lepide to list all users with passwords set to never expire so that you can reduce your overall threat surface.

Visit: Lepide Active Directory Auditing

5. Permission changes.

📊 Key Statistics

Frequency of Permission Changes in Organizations:

- A report from Varonis in 2024 highlighted that 37% of organizations experience a significant number of permission changes within their Active Directory environments each year. This includes changes such as users being added or removed from groups, modifications to file and folder access permissions, and adjustments to administrative rights.

Security Incidents Linked to Permissions Changes:

- According to a study from IBM, improper permission settings or unauthorized permission changes were responsible for 25% of data breaches in organizations, underlining the critical importance of properly managing permissions and group memberships.

⚠️ Associated Risks

Privilege escalation and lateral movement:

Improper or unauthorized permission changes are a key contributor to privilege escalation in an organization's IT environment. When users are granted permissions to sensitive resources with little oversight, a user's access to critical systems, applications, and data may become compromised. For instance, adding a standard user to an admin group (either intended or by mistake) could allow that user to perform a function that is not intended, as extreme as modifying system settings or reading confidential files or even installing malware. Cyber attackers will take advantage of misconfigured privileges as a way to escalate their privileges to gain a foot hold in the network allowing them to move casually through the environment and compromise even more of the organization without raising alarm.

Additionally, permission changes involving sensitive accounts like system admins and senior executives are higher risk. If an attacker changes permissions for these accounts, they can likely bypass other security layers and potentially assume full control over the whole system/network. Many organizations do not actively monitor changes in permissions or group memberships, so the unauthorized changes can remain undetected for long periods of time, greatly increasing the likelihood of a data compromise.

Non-compliance and audit failure:

Several regulatory frameworks like GDPR, HIPAA, SOX, and PCI DSS, stipulate that organizations must enforce strict controls over user access and permission with periodic reviews to demonstrate compliance. Excessive, untracked, or improper

5. Permission changes.

⚠️ Associated Risks (continued)

changes to permissions heighten the chance of breaching compliance. Further, if we are not logging or periodically checking permissions, we're potentially exposing ourselves towards undetectable violations that would not allow us to correct the oversight, which could lead to both reputation and monetary fines in the event of an audit.

Alternatively, improper permissions create a cascade of problems in internal audits. If there are improper permissions or over-permissioned accounts for reports in Active Directory, it can inhibit our ability to show compliance during an audit process, especially when an external evaluator must verify access controls. Even if the security practitioner wants to follow best, their own, or even documented company policy, lack of consistency in modifying permissions and a lack of proper record keeping, can contribute to an organization's inability to pass audits or comply with industry policies or standards.

Data leakage and insider threats:

Changes to permissions, especially changes that are involved with access to Confidential data, can dramatically change the likelihood of data leakage. Accesses (e.g., to shared files by a group of which one employee is no longer a part) can be misused by the employee retain those permissions (either by design, misperception , or chance) and potentially leak sensitive information, whether it is accidental file sharing, incorrect handling of information, or straightforward malice. The risk extends when users are transferring from one group or role to another group or role without reviewing their permissions based on their existing accesses.

Insider threats pose a particularly serious risk when it involves permission changes. Malicious insider threats may take advantage of existing permissions or unauthorized permission changes could provide them access to data/systems (previously not available). Additionally, changes in job roles are common within corporations, where only access privileges that adhere to their new job role should remain. Ensuring that employees/contractors only retain the appropriate level of access or permissions is paramount in mitigating the risk of involuntary or voluntary data loss breaches.

🛡️ Mitigation Strategies

Implement least privilege access and regular permission reviews:

To minimize the chance of privilege escalation and lateral movement, organizations should allow users the absolute minimum permissions necessary to complete their duties. If a user account is compromised, the overall damage will be minimized. Organizations should also implement a policy to perform regular permissions audits, a process to ensure that individuals have been assigned permission at least on quarterly basis and annually based on the type of organization to certify users have access to only necessary permissions for the performance of their duties.

Regularly reviewing group membership and role-based access control (RBAC) reduces the chances of inadvertently discovering what users possess unnecessary or excessive permissions. The review process will also include verifying certain individuals in sensitive roles possess the appropriate amount of access or no access at all. There are also tools on the market today that can help you discover and enforce least privilege, automate access control or use privileged management software, which greatly reduces human error.

5. Permission changes.

🛡️ Mitigation Strategies (continued)

Monitor and log permission changes in real-time:

Monitoring permission changes is vital for identifying and augmenting a response to unauthorized access attempts. Examples of potentially unauthorized changes might include adding a user to an administrative group, or unauthorized changes are made to a resource deemed sensitive, such as internal files related to intellectual property. Employing automated systems, like SIEM systems, to assist in discovering anomalous behavior. Identifying changes that are flagged as needing further examination or changes that fall outside the behavioral pattern established for an entity.

Establishing real-time alerting systems can also mean that your IT teams will receive alerts when certain critical permission changes are made and can act quickly to counter a potential breach. If IT is monitoring and logging permissions changes in real-time, they will be able to continuously track permission changes, and can therefore investigate any incidents and maintain an audit trail to support ongoing compliance requirements.

Use Role-Based Access Control (RBAC) and automated workflows:

Role-Based Access Control (RBAC) provides users with access based on their officially defined roles associated with the user account. The roles define what systems and particular type of data can be accessed by whom. This prevents unauthorized people from getting access to systems or data or having the capability to make ad-hoc changes to user permissions. RBAC also makes changes to permission easier. Since users are put into roles instead of managing permission for every user, it makes managing the permission changes simpler to do as the roles are assigned access rights for particular systems.

Moreover, depending on workflow systems to automate permission changes can reduce human error bites and ensure permission changes are made in accordance with established rules. For instance, if an employee changes job roles, workflows can ensure the employee's access is appropriately modified without requiring any human involvement. Automation via workflows can help ensure permission are correctly and consistently applied; this is especially beneficial when maintaining security for large user and group counts whilst enabling privileges.

💡 *Tip:* Use solutions like Lepide to list all users with passwords set to never expire so that you can reduce your overall threat surface.

Visit: Lepide Active Directory Auditing

6. Password Policy Changes

📊 Key Statistics

Frequency of Password Policy Changes:

- According to a 2024 survey by Ponemon Institute, 65% of organizations update their password policies at least once a year to improve security and align with changing best practices. However, 45% of organizations are still found to have outdated or weak password policies, which could leave them vulnerable to common attack methods like brute force or credential stuffing.

Compliance with Modern Password Guidelines:

- The 2023 Verizon Data Breach Investigations Report (DBIR) found that 40% of organizations do not enforce strong password policies, such as requiring passwords of sufficient length or complexity, leading to increased vulnerability. Many organizations still use default password expiration policies, which were found to be insufficient in protecting against cyberattacks.

⚠️ Associated Risks

Weak passwords and brute force attacks:

Effective changes to password policy are a critical debris in establishing stronger security, particularly in the face of continuously changing cyber threats. Organizations that do not implement changes and require account users to adhere to an effective password policies (strong passwords that are currently enforced) have a higher risk of brute force attacks, where an attacker utilizes automated tools to guess a password. A weak password policy with outdated policies allowing for short or simple passwords provides an attacker with an easier path to find account credentials and gain access to the organization.

When an organization has a poor password policy, the potential risks are compounded by a lack of password changes over time and a failure to utilize multi-factor authentication (MFA). This is particularly troublesome with a highly privileged account that gives the attacker the potential ability to escalate their privileges and gain access to critical systems or sensitive data.

Credential stuffing and data breach risks:

Another major risk of insufficient password policy updates is the increase likelihood of credential stuffing attacks where cybercriminals use previously compromised credentials from other services to access an account. Many individuals use the same passwords across multiple sites making it simpler for cybercriminals to compromise stolen login information. If the organization has weak password policies or no enforced changes, they are an attractive target for these types of attacks.

6. Password Policy Changes

⚠️ Associated Risks (continued)

Organizations that have very weak password policies could also be found to have violated the minimum standards set by a regulatory body (like GDPR, SOX, PCI DSS) which will require organizations to have applicable policies in place to ensure that user passwords are strong and changed often. In this case, organizations that are not updating their password policies could face legal implications and financial sanctions if their passwords do not meet these compliance standards - that could be punishable by law. According to various data breaches, password reuse and a lack of password complexity can cause the failure of sensitive customer information.

Employee resistance to frequent password changes:

Regularly changing passwords is an important security practice, but it can also create user fatigue or user resistance, particularly if policies are very complex or frequent. Employees may face difficulty remembering the increasingly complicated passwords or the short schedule for resetting passwords, and may then adopt at-risk practices, such as writing passwords down, using the same password for multiple accounts, or simply selecting simpler passwords that they find easier to remember.

The conflict of strong security practices over usability can result in workarounds that ultimately compromise the security posture of the organization. If the password-changed frequency is too frequent or overly-complex guidelines are required, then employee may take shortcuts that lessen the security of the passwords, such as identifying passwords based on identifiable phrases or names.

🛡️ Mitigation Strategies

Implement strong password policies with sufficient complexity and length:

Passwords should be long, at least 12 characters, and complex with uppercase and lowercase letters mixed, numbers, and special characters, to make them harder to guess. Moreover, accounts should be checked against lists of common passwords, so users will not pick passwords that are guessable. This type of enforcement helps ensure that even if an attacker attempts a brute force attack or dictionary attack, their success will be more difficult as the passwords will be less guessable and harder to crack.

For security purposes, organizations will typically enforce periodic password changes every 60 to 90 days. While the frequency of password changes is important for security purposes, it should be incorporated into the information security program with user fatigue and poor password practices in mind. It may also be worthwhile to recommend implementing a password manager for employees to use to make it easier for users to have access to safe and complex passwords.

Incorporate Multi-Factor Authentication (MFA):

Multi-Factor Authentication (MFA) adds a layer of security beyond requiring a password to access sensitive systems. To confirm their identity, users must provide something more than a password for the account. While MFA is generally a password (something they know) and a token (something they have, i.e., mobile device) even if an attacker is able to access the password, the attacker cannot access the account without MFA.

6. Password Policy Changes

Mitigation Strategies (continued)

For administrator and high-privilege user accounts that provide access to sensitive systems or data, implementing MFA can be critical. While lower-risk user accounts may not require MFA, it is always good practice to implement MFA for accounts that have access to critical infrastructure or sensitive data. The use of strong passwords combined with MFA provides an additional security measure and offers a strong deterrent against the successful completion of credential stuffing or brute-force attacks.

Educate employees and promote password hygiene:

Even the best password strategies can be made ineffective if the employee is not practicing basic password hygiene. Regular and consistent training and awareness for the employee is important to truly make sure the user is aware of the need for strong passwords and the possible repercussions of poor passwords. Users should be informed to avoid password reuse, how to make a strong password if required, and through education and tools (password manager) to keep any password or credential complex and safe.

Equally, it is important to ensure password change policies do not bury the user in requirements. A reasonable balance of securitizing an account and usability for the user will lower user dissatisfaction with password changing. Employees should be directed to use a password manager to generate unique, strong password for each service and periodic reviews of policies will help support they are current, not a burden to the user, and align with industry standards.

💡 *Tip:* Use solutions like Lepide to audit and report on all changes to password policies. Enable real time alerts to respond quickly.

Visit: Lepide Active Directory Auditing

7. Failed Logons

📊 Key Statistics

Prevalence of Failed Logon Attempts:

- According to a 2024 report by CrowdStrike, failed login attempts are one of the most common indicators of cyberattack attempts, with approximately 30% of organizations experiencing a significant number of failed logon attempts daily. These attempts often occur in bulk and are a key sign of an attack, such as brute force, password spraying, or credential stuffing.

Impact of Failed Logons on Security Incidents:

- The 2023 Verizon Data Breach Investigations Report (DBIR) revealed that failed logon attempts are linked to nearly 40% of data breaches involving external actors. Often, these failed attempts signal attempts to crack user passwords or gain access through unauthorized means, such as exploiting weak or compromised credentials.

⚠️ Associated Risks

Brute force and credential stuffing attacks:

Failed logon attempts can be associated with brute force attacks, which occur when cybercriminals attempt to gain access to a user's account by guessing various combinations of username and password until they find a match. If there are no controls on failed logon attempts, a brute force attack would allow an attacker to generate as many failed logins as they want until they compromise the account. Therefore, an increasing number of failed logins could be the result of cybercriminal's attempting to use common or stolen credentials.

Credential stuffing is yet another method of attack that is also tied to unsuccessful logon attempts. Credential stuffing is when an attacker reuses stolen credentials from compromised sites to attempt to access an organizations system. Attackers are able to credential stuff when users have reused passwords across platforms and have breached sites where users use the compromised credentials to try and log in. These attacks can lead to data breaches (mainly if the sensitive systems or data doesn't utilize MFA or account lockout).

Account lockouts and service disruption:

Yet another risk associated with repeated failed logons is account lockouts. This loss of access can happen for legitimate users too. A lot of systems have automatic lockout features after a certain number of failed login attempts as a way to try to limit brute force attacks. While this could deter an attacker from having success in gaining access, it also can affect legitimate users, especially if they forget their credentials or just enter them incorrectly multiple times.

7. Failed Logons

⚠️ Associated Risks (continued)

In addition, we may see the denial-of-service scenario happen due to high failed login attempts. For instance, an attacker could send a large amount of failed login attempts to the organization's system and drain its resources, slowing it down or even taking it offline. In this scenario, the attacker will likely perpetrate failed login attempts as they may want to overload the organization's systems. This could seriously disrupt the organization's business and continuing continuity.

False sense of security and lack of monitoring:

When organizations do not monitor or analyze failed logins, they may be creating a false sense of security. It's not enough to establish a maximum threshold of failed logons before account lockout. Monitoring failed logins and providing real-time alerts will help the IT team identify attempts to conduct brute force or credential stuffing attacks. Failed logon attempts can take place for days, weeks, or months before detection can happen and they can be successfully followed by attackers. Failure to track failed attempts and identify the attempts before their successful entry allows the malicious actor to operate blindly against a critical system.

In addition, missing intelligent logging and correlation may lead teams not to see pivotal warning flags For instance, if failed logons are being tracked in isolation without a broader view of the network's behavior or threat landscape, it may be harder to distinguish legitimate user errors from actual attack attempts. Monitoring failed logon attempts, along with contextual data like the time of day, geographical location, and source of requests, is essential to detect and block malicious activity proactively.

🛡️ Mitigation Strategies

Implement Multi-Factor Authentication (MFA):

One of the best methods to safeguard against unsuccessful logon that grants unauthorized access is to use multi-factor authentication (MFA). MFA asks users to give something they possess (e.g., a smartphone, hardware token, or biometric scan) and something they know (a password). Even if the attacker is able to steal or brute-force a user's password, they will still need the second factor in order to be able to access the system. This serves to significantly reduce the risk of successful attack, even when there are repeated failed attempts at login.

MFA is particularly vital for high-privilege accounts, such as system administrators because they provide higher levels of access to mission-critical systems and highly confidential data. By implementing MFA, organizations can add a robust level of security against credential-based attacks.

Implement account lockout and rate-limiting policies:

Organizations should configure their systems to automatically lock accounts after multiple failed login attempts—three or five failed attempts—so as to prevent brute force attacks. While it may prevent illegitimate login attempts, it should be ensured that the lockout duration is not so long as to be inconvenient for legitimate users. An automatic lockout policy can also be used together with a brief cool-off period prior to the users being allowed to try again, or even more advanced reCAPTCHA-style authentication in order to prevent login attempts by a bot over a human.

7. Failed Logons

Mitigation Strategies (continued)

In addition to this, organizations should also implement rate-limiting policies to restrict the number of login attempts per minute or hour from a single IP address. This slows down the automatic attack that relies on the use of high volumes of login attempts and can minimize the impact of an attack by slowing down the brute force or credential stuffing attack.

Monitor and analyze failed login attempts in real-time:

Monitoring failed login attempts in real-time is central to attempt attack detection and response on time. Organizations must configure their systems to notify the IT teams in case a predetermined number of failed logins has been attempted, or there has been an attempt to login from a suspect IP address or device. Security teams can detect malicious patterns of activity through relating the above data with other security parameters including IP geolocation, time, and historical successful logons.

Tools like Security Information and Event Management (SIEM) systems can be employed to collect, analyze, and alert on failed login information. The systems can be utilized to discover trends and anomalies in the failed login information that can indicate an ongoing attack and allow the organization to take speedy action and stop further intrusion. Constant monitoring of login activity is also valuable for identifying patterns over time that may signal deeper security problems, including users with weakly guessed passwords or duplicate credentials on multiple accounts.

💡 *Tip:* Use solutions like Lepide to set threshold alerts for when a large number of failed logons are experienced in a short space of time, indicating a brute force attack.

Visit: Lepide Active Directory Auditing

8. Account Lockouts

📊 Key Statistics

Prevalence of Account Lockouts:

- A 2024 study by CyberArk found that 55% of organizations have experienced account lockouts at some point, with many of these lockouts being triggered by failed login attempts. 45% of businesses report that they struggle to balance lockout policies with employee productivity, especially when legitimate users are frequently locked out due to incorrect login attempts.

Frequency and Impact of Lockouts:

- According to a report by Rapid7, 43% of organizations report frequent account lockouts, leading to substantial downtime and administrative burden. The report highlights that these lockouts can significantly disrupt workflows, particularly if users are unable to quickly regain access to their accounts.

⚠️ Associated Risks

Disruption of business operations:

While account lockouts are an excellent tool against brute force attacks, they can also be bothersome for legitimate user access to security-sensitive systems, especially when there are excessive failed login attempts and temporary or permanent account lockout. For example, employees are locked out of their accounts because they forgot their passwords or when security auto-features inadvertently label their login activity as malicious. This can result in downtime and affect productivity, particularly if the users must regain access to business-critical applications quickly.

In a high-risk business situation, such as in healthcare, finance, or critical infrastructure industries, being unable to access systems because of account lockouts may be more than just inconvenient—it can have critical business repercussions. For instance, locked-out users may be barred from viewing patient records, financial details, or other confidential data, disrupting workflows and decision-making processes. The administrative burden on IT staff to terminate such lockouts adds to the expense of operations, and in the event that it is not managed well, such disruptions can affect customer satisfaction and general organizational performance.

Potential for account lockout abuse:

Malicious users can intentionally initiate account lockouts as a Denial of Service (DoS) attack to disrupt an organization's operations. The attack, also known as account lockout denial of service, is executed by bombarding a system with numerous failed logins to lock out multiple users, causing huge disruption. This attack is most harmful to organizations whose business completely relies on some applications or user logins for daily operations..

8. Account Lockouts

⚠️ Associated Risks (continued)

Attackers also take advantage of weak lockout policies that do not put in place adequate countermeasures. For example, an attacker may attempt several logins using a list of weak or stolen passwords, leading to several account lockouts. In case the lockout threshold is too low or lockout duration too long, attackers can exploit these vulnerabilities with the aim of hindering business functionality, overwhelming the authentication systems, or even denying legitimate users access to essential resources.

False sense of security:

While account lockouts can reduce brute force attacks, they are not a complete security solution. They can create the illusion of being secure by deterring attackers from accessing in plain brute force but fail to address other attack modes, such as social engineering, phishing, or insider attack.

Additionally, account lockouts alone may not be sufficient to prevent advanced attacks. Advanced attackers are able to use more advanced methods such as credential stuffing or password spraying, whereby they use known username and password pairs on numerous accounts without triggering lockout thresholds. In these cases, although no individual account is locked, unauthorized access could indeed be achieved by attackers. Without complete, advanced security technologies, reliance solely on account lockouts could lead to an attitude of complacency in organizations.

🛡️ Mitigation Strategies

Combine account lockouts with Multi-Factor Authentication (MFA):

To better secure accounts, organizations can implement multi-factor authentication (MFA) in conjunction with account lockout policies. Account lockouts prevent unauthorized access by closing out brute force attacks, but MFA offers additional security that involves users authenticating with something they possess (e.g., mobile device, hardware token) or something they are (e.g., biometrics). It significantly reduces the likelihood of attackers successfully entering accounts even if they managed to bypass the lockout feature.

For highly privileged accounts, such as those with admin privileges, it is especially critical to require MFA. Admin accounts are the most likely targets of attackers, and additional authentication factors can prevent unauthorized access even if an attacker were successful with a brute force or credential stuffing attack.

Fine-tune lockout policies to avoid overreaction:

Organizations must ensure their account lockout policies are set to reasonable levels. Locking accounts following a small number of failed logins, for example, can lead to excessive lockouts, particularly in multisite or mobile-worker settings. A more finely grained practice may be to briefly lock out accounts following a series of failed login attempts (e.g., 3 to 5 attempts), with a brief cool-down time before additional attempts are allowed. This will deter brute force attacks without unnecessarily disrupting legitimate users.

8. Account Lockouts

Mitigation Strategies (continued)

Also, it is prudent to implement logging and monitoring of failed login attempts to detect potential attacks in advance. Automatic alerts can notify IT personnel when suspicious patterns of failed logins are detected, allowing them to investigate and respond before major disruptions occur. Businesses can also investigate the use of tools like account activity monitoring software to track login attempts in real-time, flagging unusual activity and triggering more assertive response mechanisms when necessary.

Educate users and provide self-service options:

User education is essential in reducing the number of uncontrolled account lockouts that occur as a result of password entry mistakes. Training employees on good password practices, such as regularly changing passwords and avoiding common words, can decrease the risk of logon errors. Organizations must also encourage the use of password managers to help users create good, new passwords for each service they use.

Self-service password reset sites must also be made available to allow users to be restored quickly to access without IT intervention. This can assist in reducing the administrative burden on IT staff and reduce the downtime for users locked out due to forgotten passwords. By allowing users to securely self-reset passwords using identity authentication, organizations will be able to prevent lockout events from disrupting workflow for too long.

💡 *Tip:* Use solutions like Lepide to set threshold alerts for when a large number of account lockouts are experienced in a short space of time, indicating a brute force attack.

Visit: Lepide Active Directory Auditing

9. Activity Outside of Business Hours

📊 Key Statistics

Prevalence of After-Hours Activity:

- According to a 2024 study by FireEye, approximately 25% of organizations report detecting suspicious activity outside of regular business hours. In these instances, many of the activities were traced back to compromised accounts being exploited by cybercriminals during times when the business is less likely to be monitoring or responding to security threats (FireEye 2024).

Connection to Insider Threats:

- A 2023 study by Varonis found that 33% of cybersecurity incidents were caused by insiders accessing systems outside of business hours. The report highlights that insiders are increasingly exploiting after-hours access, taking advantage of a lack of monitoring during off-peak times. This behavior often signals either an attack in progress or an insider trying to cover their tracks (Varonis 2023).

Spike in Activity During Non-Business Hours

- The 2023 Verizon DBIR found that 37% of breaches occurred during non-working hours, underscoring the critical need for vigilance outside the typical business window. Attackers often exploit the fact that there is reduced human oversight and less monitoring of IT systems during evenings and weekends.

⚠️ Associated Risks

Increased risk of insider threats:

Off-hours activity is often an indicator of malicious insider threats, intentional or unintentional—by contractors or employees with legitimate access to company systems. Malicious insiders utilize off-hours activity to exfiltrate sensitive data, steal intellectual property, or destroy systems while attempting to avoid detection. Employees with access to administrative rights or high-privilege accounts might use after-hours periods to make unauthorized changes or export sensitive data outside the enterprise.

Unintentional insiders are also a risk. For example, employees might access systems outside normal working hours for convenience, such as working from home late at night, which can lead to poor security hygiene, such as logging on from an open network. If these practices are not monitored or flagged, they can increase the vulnerability to cyberattack, especially if the login credentials of the employee have been hijacked.

Attackers exploiting reduced monitoring:

Cyber attackers usually target organizations outside business hours because they think there would be lesser scrutiny and action during such periods. The lax vigilance provides the attackers with a window to conduct their attack without discovery. Should the attackers succeed in penetrating the system, the effects of the compromise during off-business hours have a tendency to be graver due to the delayed response time, giving the attackers more time to scale up the attack, spread across the network, and steal sensitive information.

9. Activity Outside of Business Hours

⚠️ Associated Risks (continued)

Attackers can use phishing or credential stuffing attacks to initially breach corporate systems. From the inside, they can continue under the radar, making lateral movements on the network to reach more secured systems, drop malware, or even disable security software before discovery takes place. The longer the attack remains undetected, the more expensive and destructive the breach. In other cases, the attackers will stay undercover, biding their time until an opportunity to attack when normal working hours bring business back.

Misuse of privileged access and data exfiltration:

Privileged accounts and access to sensitive information are generally most vulnerable to misuse outside working hours. For instance, employees who have high permission levels and access to monetary information or customer details might utilize their permissions to download, copy, or send sensitive material to off-premises accounts. With no presence of controls or limitations on the use of such privileged access off-hours, insiders can take advantage of them to conduct illicit actions without triggering alarms or security notifications.

Even when performed by authorized staff, such after-hours access can be seriously dangerous. Data exfiltration, for example, could be the outcome as sensitive business data is removed from the office on employees' personal devices or by transferring files using unencrypted methods, which could be intercepted or lost in the unsecured world outside the company's network boundary. Such information could be valuable to attackers who would exploit it or sell it for competitive advantage or ransom.

🛡️ Mitigation Strategies

Implement continuous monitoring and alerts for non-business hours:

Organizations need to have real-time monitoring solutions in place that track user activity on all systems, particularly outside of business hours. By utilizing Security Information and Event Management (SIEM) systems, organizations can collect and analyze log data to identify anomalous or unauthorized login activity outside of the standard working hours. Automated notifications should be configured to alert security teams in real time when there is unusual activity, such as logins from unknown locations, access attempts by unrecognized devices, or changes to critical systems.

Machine learning and anomaly detection features within SIEM enable it to recognize patterns that are indicative of an attack, such as logging in after hours from a different IP address than usual or trying to access sensitive data in unusual ways. Acting upon these alerts promptly, organizations are able to take proactive steps to block or quarantine the activity before the situation escalates.

Implement access controls and restrict privileged access after hours:

To minimize the danger of malicious insiders or off-hours attackers, organizations can consider implementing time-based access controls to restrict access to privileged accounts and sensitive systems outside of business hours. As an example, organizations can limit administrator account activity or superuser privileges within specified work hours. This will help grant access to only authorized people to critical systems when they are working, thus reducing the attack surface during off-work periods.

9. Activity Outside of Business Hours

Mitigation Strategies (continued)

Also, least privilege access needs to be enforced so that the users can have access only to the systems and data they need for their work to restrict the damage in the event of stolen credentials. Organizations have to review and strengthen their privileged access management policies periodically so that the privilege of users to have access is aligned with their role and responsibilities.

Educate employees and raise awareness about after-hours security risks:

Employee training is a critical element of any security plan. Training on security awareness must include education on how off-hours access can represent a security threat, particularly when employees are working from home or on personal computers. Employees need to be trained on the importance of following secure login protocols, such as using good, unique passwords, not logging into work-related tasks on public Wi-Fi, and using Virtual Private Networks (VPNs) when remotely accessing company systems.

Organizations must also advertise the importance of reporting suspicious off-hours activity from both legitimate users and external attackers. Through educating employees on the dangers and best practices, the likelihood of inadvertent insider threats will lessen and the security position of the organization will be improved overall.

💡 *Tip:* Use solutions like Lepide to receive real time alerts to your mobile device whenever any activity occurs outside of business hours.

Visit: Lepide Active Directory Auditing

10. User / Computer Status Changes

📊 Key Statistics

Prevalence of Account Status Changes:

- According to a 2024 report by Microsoft, 21% of organizations regularly review and update user and computer account statuses to ensure that only active and authorized personnel have access to corporate systems. However, the same report highlights that 13% of organizations fail to regularly disable or lock user accounts that are no longer active, increasing the risk of unauthorized access.

Impact of Inactive Accounts:

- The 2023 Cybersecurity and Infrastructure Security Agency (CISA) report reveals that 20% of cyberattacks stem from compromised accounts that were not properly disabled or locked after an employee left the company. This highlights the critical importance of deactivating or locking user and computer accounts immediately when they are no longer required.

Vulnerability of Disabled / Locked Accounts:

- According to the 2023 Identity and Access Management (IAM) report by Okta, over 30% of organizations have failed to lock or disable user accounts for former employees within a timely manner, creating significant risks for unauthorized access and data breaches.

⚠️ Associated Risks

Unauthorized access from inactive or disabled accounts:

One of the greatest threats from improperly disabled or locked accounts is that unauthorized individuals will utilize the accounts to access critical systems or data. When employees leave an organization, either voluntarily or involuntarily, their accounts remain active for far too long. This provides a backdoor entry point for attackers, who will utilize the dormant accounts for brute force or credential stuffing attacks.

Similarly, if user and computer accounts that are owned by ex-employees or contractors are not disabled correctly, attackers who gain access to these accounts can have a window of opportunity for privilege escalation, pulling out sensitive information, or installing malware. Former employees may also attempt to utilize these accounts for revenge or financial gain, particularly if they have internal system knowledge. These threats are heightened if the organization does not audit user access logs on a regular basis to detect suspicious activity involving disabled accounts.

Compromised user and computer accounts:

Inactive accounts are vulnerable to attack, particularly when they reuse or have poor credentials. The attacker can use brute force or leverage previously compromised known credentials to gain unauthorized access into the system. Once inside the system, the attacker will be able to privilege escalate, make unauthorized changes, or laterally move around the network to other more compromised systems or accounts.

10. User / Computer Status Changes

⚠️ Associated Risks (continued)

This risk is exacerbated by poorly managed account lifecycles, where new accounts are provisioned for users with insufficient oversight and existing accounts are never deactivated. Once an account is hijacked, it can become a long-term attack vector that enables attackers to perform activities below the radar and cause serious harm. In some cases, attackers have been known to use dormant computer accounts to bypass network security controls or use them as a launch point to deploy malware or ransomware attacks.

Compliance and regulatory violations:

Certain sectors are governed by rule of compliance (e.g., GDPR, HIPAA, PCI DSS) where companies are requested to disable or lock accounts for departing employees or contractors. Failure to do it can lead to non-compliance and immense fines. Moreover, extended access via dormant or disabled accounts can lead to violation of privacy if sensitive information is accessed or extracted by unintended users.

This is especially the case in industries like healthcare and finance, in which personal data is of sensitive nature. Organizations need to follow strict data accessibility and retention guidelines, and providing former employees or unauthorized users with access to systems could result in severe reputational damage and legal consequences. Regular reviews and updates of user and computer account statuses might guarantee compliance and eliminate such risks.

🛡️ Mitigation Strategies

Implement automated user account deactivation and review:

Maybe the most effective way to minimize risks stemming from inactive or disabled accounts is to automate the deactivation. Businesses can set up systems that automatically block or disable unused accounts for a specified time period, e.g., 30 or 60 days. This can be done via identity and access management (IAM) software or user lifecycle management products, which are able to flag de-active accounts and revoke access to systems upon automatic termination when employees leave the organization.

In addition, organizations can carry out automated account status checks quarterly or every year to ensure that all the accounts remain active and utilized. Using automated reporting tools, organizations are able to identify inactive accounts and disable them promptly. This avoids unused or unnecessary accounts remaining open and provides a convenient way of attaining data protection and privacy compliance.

Enforce strong access control policies and periodic audits:

Organizations have to establish a strong set of access control policies that entail overt procedures for disabling user accounts once employees are terminated, leave the company, or do not need access to specific resources anymore. This should include timely disabling of accounts, even for temporary employees or contractors, once they end their relationship with the organization. Access needs to be reviewed regularly for employees in critical positions so that only the staff members who need to access critical systems are given such access.

10. User / Computer Status Changes

Mitigation Strategies (continued)

In addition, recurring access audits must be conducted to identify any unused, inactive, or inactive accounts. These audits can help organizations identify accounts previously missed during audits and ensure compliance with external and internal security policies. Audit logs can also provide visibility into whether unauthorized activity has been performed on such accounts.

Educate employees and IT teams on account lifecycle management:

Staff training is important in order to guarantee proper management of user accounts during their lifecycle. The organization needs to train the HR staff and IT staff on following a standard and safe process of creating, updating, and deactivating accounts. This entails having proper procedures for managing employees leaving the company, including canceling their access promptly and securely.

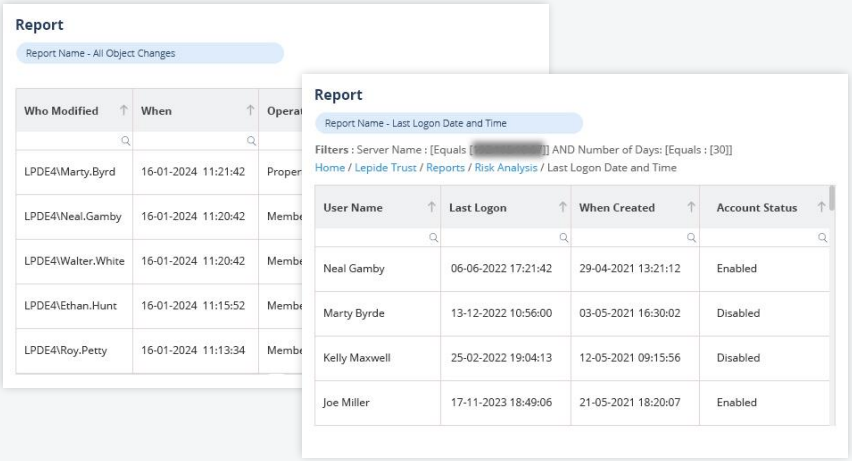
Staff should also be taught the importance of good password hygiene and locking personal devices in the event they are remote-accessing corporate systems. Training IT staff on how to effectively audit account behavior and detect unusual patterns related to inactive accounts will do much to prevent risk from compromised credentials. Security campaigns aimed at the threats of account reuse and insider threats can also reduce the likelihood of accounts being open or exploited.

💡 *Tip:* Use solutions like Lepide to receive real time alerts to your mobile device whenever any activity occurs outside of business hours.

Visit: Lepide Active Directory Auditing

How Lepide Can Help Simplify AD Security.

Lepide Auditor for Active Directory provides detailed audit trails with the critical “who, what, where, and when” audit information for all Active Directory changes and events. Lepide provides detailed state-in-time Active Directory security audit reporting so admins can fully understand what their AD looks like. Lepide also tracks user behavior, including logon/logoff behavior and account lockouts.



💡 Learn more about how Lepide can help you simplify your Active Directory auditing and security.

Visit: Lepide Active Directory Auditing

Complete audit trail for all events/changes.

Get before and after values of every change with the answers to the who, what, when and where questions through 100+ audit reports.

Detailed account lockout analysis.

Easily identify the source of account lockouts (processes, tasks, services, etc.) and unlock accounts from within the platform.

Track and report on logon activities.

You can easily audit failed logon events, concurrent logon sessions, users' login history on to multiple computers and much more.

Analyze effective and historic permissions.

Analyze the effective permissions of your users and spot permission changes. Reverse unwanted permission changes to an ideal state.

Rollback unwanted changes.

Rollback unwanted or unplanned change to original values. Even lets you retrieve objects from tombstone and recycled state.

Audit Group Policy events and changes.

Track modifications made to Group Policy objects and proactively thwart any alterations to the most vital GPOs.

Cited Sources

1. **Statista – Number of Microsoft Active Directory Users Worldwide**
   Statista provides data on the widespread use of Microsoft Active Directory, detailing its adoption across enterprises worldwide.

2. **Gartner – The State of Identity and Access Management in 2023**
   Gartner's research highlights trends in identity and access management, including the increasing scale of user bases within organizations and the related complexities.

3. **Kaspersky – The Global Cybersecurity Landscape 2024**
   Kaspersky's cybersecurity report discusses various factors affecting IT environments, including the growing numbers of user accounts in large organizations and the associated security risks.

4. **Security Awareness – The Security Risks of Over-Privileged Accounts**
   A report discussing the dangers of over-privileged accounts in AD, especially in organizations with large user bases.

5. **Microsoft Learn – Best Practices for Securing Active Directory**
   Offers guidance on best practices for securing Active Directory, including account management strategies.
   Microsoft Learn

6. **Microsoft Learn – Review and Reduce the Number of Accounts in Highly Privileged Administrative Groups**
   Discusses the importance of reviewing and reducing highly privileged accounts in Active Directory for better security.
   Microsoft Learn

7. **Frame Secure – The Risks of Excessive Admin Privileges**
   Explores the risks posed by excessive admin privileges in Active Directory environments and the need to control access.

8. **Infosecurity Magazine – Too Many Admins: Admin Privileges Run Rampant Across Organizations**
   This article highlights the widespread issue of excessive admin privileges in organizations and the associated risks.
   Infosecurity Magazine

9. **Windows Active Directory – Securing Administrator Accounts in Active Directory**
   Best practices for securing administrator accounts in Active Directory, focusing on preventing privilege escalation and securing sensitive access.
   Windows Active Directory

10. **Varonis – Active Directory Security: The Silent Danger of Inactive Accounts**
    Varonis discusses the growing number of inactive accounts in large organizations and provides insights on securing Active Directory environments.
    Varonis

11. **Verizon 2023 Data Breach Investigations Report (DBIR)**
    Verizon's report details how breaches often result from the failure to properly disable accounts, especially those that are inactive or tied to former employees.
    Verizon DBIR 2023

12. **CISA 2023 – Cybersecurity Best Practices for Account Management**
    CISA's report highlights the need for timely disabling of accounts tied to former employees to prevent security breaches.
    CISA 2023

13. **Okta 2023 – The Importance of Account Lifecycle Management**
    Okta's study discusses the importance of account lifecycle management, including the timely deactivation of accounts to mitigate risks.
    Okta 2023

Lepide

The State of Active Directory Security:

Key Risks to Monitor for 2025

https://www.lepide.com